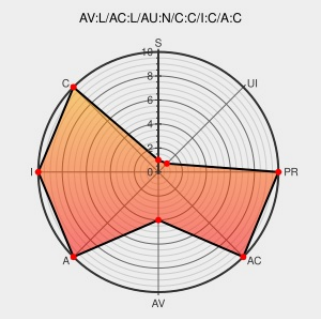
CVE-2005-3581

Published on: 11/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-3581

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gdal from Gdal contain the following vulnerability:

GDAL before 1.3.0-r1 allows local users in the portage group to increase privileges via a shared object in the Portage temporary build directory, which is added to the search path allowing objects in it to be loaded at runtime.

CVE-2005-3581 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 20529
Gentoo update for qdbm / imagemagick / gdal - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 17427
Gentoo Linux Multiple Packages Insecure RUNPATH Vulnerability	cve.report (archive) text/html	BID 15120
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2281
Gentoo Linux Documentation -- QDBM, ImageMagick, GDAL: RUNPATH issues	Patch Vendor Advisory	GENTOO GLSA-200511-02

www.gentoo.org
text/html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gdal	Gdal	1.2.5	All	All	All
Application	Gdal	Gdal	1.2.5_r1	All	All	All
Application	Gdal	Gdal	1.2.6_r1	All	All	All
Application	Gdal	Gdal	1.2.6_r2	All	All	All
Application	Gdal	Gdal	1.2.6_r3	All	All	All
Application	Gdal	Gdal	1.2.6_r4	All	All	All
Application	Gdal	Gdal	1.3.0	All	All	All
Application	Gdal	Gdal	1.2.5	All	All	All
Application	Gdal	Gdal	1.2.5_r1	All	All	All
Application	Gdal	Gdal	1.2.6_r1	All	All	All
Application	Gdal	Gdal	1.2.6_r2	All	All	All
Application	Gdal	Gdal	1.2.6_r3	All	All	All
Application	Gdal	Gdal	1.2.6_r4	All	All	All
Application	Gdal	Gdal	1.3.0	All	All	All

cpe:2.3:a:gdal:gdal:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.5_r1:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r1:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r2:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r3:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r4:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.5_r1:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r1:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r2:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r3:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.2.6_r4:*:*:*:*:*:*:*:

cpe:2.3:a:gdal:gdal:1.3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→